MINUTES IACR BOARD MEETING *VIRTUAL-1 ’19*

13 MARCH 2019

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 15h03 CET Cachin opens the virtual meeting over Zoom videoconference and he briefly goes around confirming attendees.

1.2. **Review and approval of agenda.** The agenda is approved, with the understanding that the meeting will be held in an order slightly deviating from the agenda (as certain items have scheduling constraints). These minutes are reordered to the original agenda for consistency.

1.2.1. *Roll of Attendees.* There are 19 full time attendees. Standaert joined the meeting at 16h00 CET while Kim leaves the meeting at 16h00 CET and Bos leaves at 16h30. Stebila takes the minutes for the last half hour of the meeting.

The President welcomes the new Board members: Heninger, Batina, and Kim.

Attendees (Elected). Christian Cachin (President 2017-2019); Brian LaMacchia (Treasurer 2017-2019); Joppe Bos (Secretary 2017-2019); Michel Abdalla (Director 2019-2021); Masayuki Abe (Director 2018-2020); Shai Halevi (Director 2017-2019, *TCC* Steering Committee); Nadia Heninger (Director 2019-2021); Tancrède Lepoint (Director 2018-2020); Anna Lysyanskaya (Director 2019-2021); Francois-Xavier Standaert (Director 2017-2019, *CHES* Steering Committee); Moti Yung (Director 2018-2020, *PKC* Steering Committee).

Attendees (Appointed). Lejla Batina (*Eurocrypt’20* General Chair 2019-2020); Marc Fischlin (*Eurocrypt’19* General Chair 2018-2019); Kwangjo Kim, (*Asiacrypt’20* General Chair 2019-2020); Kenny Paterson (Journal of Cryptology Editor-in-Chief 2017–2019, *RWC* Steering Committee); Douglas Stebila (Membership Secretary 2017-2020); Muthu Venkitasubramaniam, (*Crypto’19* General Chair 2018-2019).

Attendees (Representatives and Others). Tal Rabin (Code-of-conduct Liaison); Kevin S. McCurley (Database Administrator);

Absentees (Elected). Greg Rose (Vice President 2017-2019); Bart Preneel (Director 2017-2019, *FSE* Steering Committee);

Absentees (Appointed). Leo Reyzin (*Crypto’20* General Chair 2019-2020); Mike Rosulek (Communications Secretary); Mitsuru Matsui (*Asiacrypt’19* General Chair 2018-2019);

Absentees (Representatives and Others). Hilarie Orman (Archivist); Yu Yu (Webmaster); Marc Rotenberg (General Counsel);

2. Appointments, committees and policies

2.1. **Ethics committee.** The President recalls that the Ethics Committee needs a replacement for Rogaway. Heninger volunteers and there are no objections.

2.2. **Election committee.** The President recalls that he will not be running for this position next year but will chair the Election Committee. He calls for volunteers whose position are not up for election next year. Both Lepoint and Abe volunteer to joing the Election Committee and there are no objections.

2.3. **Communications secretary.** The President explains that Rosulek wants to step down as Communications Secretary. We are not ready to announce a replacement and he asks the Board for suggestions. McCurley is willing to step in for web development skills for the Communications Secretary which might ease finding the right profile.

Action Point **1: Cachin** *(Board Meeting at Eurocrypt’19)*:
Find candidates for the position of Communications Secretary

2.4. **JoC Editor-in-Chief.** The President thanks Paterson the tremendous great job he has been doing as the JoC Editor-in-Chief. Paterson explain that he does not want to be re-appointed for another 3-year term. However, he is willing to do one additional year making his term a 4-year one. There are no objections from the Board.

Action Point **2: 2020 IACR President** *(no time set)*:
Find a new JoC Editor-in-Chief

3. Budget and financial

3.1. **IACR Budget 2019.** The Treasurer presents the Treasurer's Report and the FY18 Financial Highlights. He explains that the major income sources are USD 252K overall upside from conferences and almost USD 100K from membership. The major IACR expenses are USD 60K for student speaker stipends and USD 40K for IACR Schools. Due to the TransferWise account the currency conversion cost (Euro to USD) has dropped from 3 to less than 0.4 percent. The idea is to use non-conference income for schools, student waivers and conference support.

The Treasurer moves on to explain the FY19 Profit & Loss Budget Overview and proposes to set aside a budget to support conferences to lower the registration fees. There follows a discussion about the conference support and how that works in practice. Lepoint wonders if a change in registration fee of USD 20 really matters compared to the cost of the entire trip. He suggests to use this budget to increase the student support even further. Halevi thinks this budget is a good idea since it is an incentive for the General Chairs not to bee too conservative. Abdalla remarks that for the General Chairs it is often very difficult to correctly estimate the number of attendees. The Treasurer explains that it is up to the General Chair how to use any leeway. The President states that the student support should already be in the budget for the conference.

There follows a discussion about waivers for non-student speakers. Halevi and the Treasurer wonder if we should also include funding travel cost. The President expresses that a lower fee for everyone has its advantages. Stebila prefers to use this budget set aside by the Treasurer to get more students; the excess income from last year could be used to reduce the conference registration fees. The President supports this proposal by Stebila.

Action Point **3: LaMacchia, Stebila, Cachin** *(Board Meeting at Eurocrypt'19)*:
Work out the proposal to lower the registration fees and fund more student from excess income from last year.

The President asks about the USD 12k cost for the JoC while the income is only USD 3k. The Treasurer recalls that the USD 3 is to cover the mailing cost while the remainder is the cost for the submission server. McCurley asks about the cost for Transactions of CHES and Transactions on Symmetric Cryptology. The Treasurer explains that as far as he is aware there is no cost to these transactions.

The President thanks the Treasurer for his great work.

3.2. **Schools funding 1H2019.** Abdalla summarizes the report which was shared before the meeting. The Schools Committee received a total of two proposals in this latest round. One proposal asks for a significant amount of budget (over USD 60k) with a very broad topic and the Committees proposal is to not support this one. The second proposal is a summer school on Euclidean lattices in Russia and asks for EUR 4k. The Committee recommends to fund this proposal.

Lysyanskaya expresses concerns with such a school in Russia and is worried about the organizers of this event. Stebila highlights that it is good to support research communities around the world, we don't have sufficient information to judge the safety of the organizers.

Decision 1. *The Board decides to follow the recommendation of the Schools Committee and fund the summer-school proposal in Kaliningrad, Russia.*

4. Topics

4.1. **Journal-first track for IACR General Conferences.** Halevi explains the proposal for the journal-first track for IACR General Conferences. He explains that the timeline for this proposal is not clear yet. One idea is to have the submission deadline 4 months in advance of the conference. One potential problem is to find good reviewers, could we rely on the Program Committee members? Abdalla wonders if we could limit the number of papers for this track. Abe raises the concern what would happen if we receive too many submissions. Paterson explains that the idea is to introduce this incrementally and be flexible with the deadline. Heninger shares her experience that multiple deadlines per year might result in a significant increase of submission.

There follows a discussion how to publish these papers in the conference proceedings and if this is compatible with the current publisher contract. The President states that it would be good to clarify answers to the various questions raised. However, it would still be good to have an opinion of the Board on the general procedure. Paterson notes that the PCs of conferences may be unhappy as this cedes some power over the program to the JoC.

Yung notes concerns about competing papers that come on different tracks. Paterson says eventually PCs would be appointed with this understanding at appointment time.

Yung says we need to think this better through and address possible corner cases. Paterson volunteers to work with Halevi on fleshing out a proposal. Halevi requests that the Board indeed send emails to Paterson and himself about such corner cases. Yung already mentions a few including merging papers, and journal papers not making it through a first deadline but then a conference paper coming in between. The President notes we would also need to involve Program Chairs and possibly Springer.

Decision 2. *The Board recommends the JoC Editor-in-Chief to develop a more detailed proposal on the journal-first track.*

Action Point **4: Paterson, Cachin, Halevi** *(Board Meeting at Eurocrypt'19)*:
Consult PCs and revise the current proposal for the journal-first track.

4.2. **Petition on US visa issues.** Lepoint wonders why we are considering a petition and not an IACR statement. LaMachia states that we as the Board can adopt a position directly. Lysyanskaya asks if we can find out what happened to Shamir via an Freedom of Information Act (FOIA). Stebila states that many people beyond Shamir have problems with visa issues, so our statement could be broader than the circumstances of Shamir's rejection. Abe mentions that this does not only happen to people from countries we named so far but also to a lot of Japanese researchers.

The President asks the Board if they have suggestions how to proceed. Yung suggests that the Board submits a general letter. Hosting crypto conferences in the US is to the benefit of the US. Lysyanskaya wants to get to the bottom of things: Only way to find out if we are we singled out for doing cryptography is by FOIA. Cachin believes doing one does not exclude the other. McCurley believes the issue is broader than cryptography and applies to other sensitive areas as well. Halevi states that FOIA may or may not give us something, but we might as well make a FOIA request any way. We should task a Board member to investigate with other areas of CS to see how widespread this is.

The President sees potential action items for a statement, the FOIA, and investigating other areas. Lepoint request to vote on the action(s) the Board should take.

Decision 3. *The Board decides to draft a statement addressing the US visa issues.*

A motion regarding coordinating with individuals to submit a FOIA fails. Cachin suggests that those interested could pursue this individually. The President seeks volunteers to help with statements. Members of the Board are encouraged to investigate FOIA, but IACR does not have the resources to do this at this time.

Action Point **5: Cachin** *(no time set)*:
Appoint someone who will take the lead in drafting a statement addressing the US visa issues.

4.3. **Arxiv.org, including relation to eprint.** Cachin summarizes the e-mail that was circulated before the meeting regarding the request to the IACR to nominate a person for the editor position in cryptography and security for the CS branch of Arxiv.org. The President is unsure whether we are ready to recommend names at this point in time. Cachin suggests we need a broader discussion, unless we have a strong candidate now. No suggestions from the Board are provided. Lepoint notes we should definitely respond about recommending someone.

Action Point **6: Cachin** *(no time set)*:
Collect names and then respond to the e-mail about recommending an cryptography and security editor for Arxiv.org.

4.4. **Eurocrypt 2019 update.** Fischlin provides an update on *Eurocrypt'19* and reports that registration has been opened. Cachin remarks that no e-mail was sent announcing registration is open. Fischlin summarizes his report. Fischlin would like the Board to clarify how workshops are viewed – are they part of the conference, does IACR get to approve chairs, what if chairs don't do their work? Cachin asks Marc to make a list of workshop issues that come up, and then the Board can evaluate these.

Cachin thanks Fischlin and looks forward to *Eurocrypt'19*.

4.5. **Web modernization.** McCurley summarizes the report on web modernization he circulated before the meeting. Cachin thanks McCurley and McKelly for all the work that they have been doing.

Cachin closes the virtual meeting at 17h02 CET.